Practitioner's Docket No. NAI1P002/00.056.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lee Benzinger et al.

Application No.: 09/586,550 Group No.: 3624
Filed: 05/31/2000 Examiner: Snapp, Sandra
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR DYNAMIC SYSTEM ADAPTATION USING CONTRACTS

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on April 21, 2004.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory;***
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

☒ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

_ facsimile transmitted to the Patent and Trademark Office, (703) _____ - _____.

Melissa D. Orvis
Signature

Date: 4/30/04

Melissa D. Orvis
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity	$330.00

Appeal Brief fee due $330.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$330.00
Extension fee (if any)	$0.00

TOTAL FEE DUE $330.00

6. FEE PAYMENT

Attached is a check in the amount of $330.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P002).

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Silicon Valley IP Group, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of: Benzinger et al.	) Docket: NAI1P002/00.056.01
Filed: 05/31/00	) Examiner: Snapp, Sandra S.
Serial Number: 09/586,550	) Art Unit: 3624
FOR: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR DYNAMIC SYSTEM ADAPTATION USING CONTRACTS	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on April 21, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. § 1.192(a))

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 1.192(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 1.192(c)(1))

The real party in interest in this appeal is Networks Associates Technology, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 1.192(c)(2))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals or interferences.

III STATUS OF CLAIMS (37 C.F.R. § 1.192(c)(3))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-7, 9, 11-17, and 19-23.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration but not canceled: None
2. Claims pending: 1-7, 9, 11-17, and 19-23
3. Claims allowed: None
4. Claims rejected: 1-7, 9, 11-17, and 19-23

C. CLAIMS ON APPEAL

The claims on appeal are: 1-7, 9, 11-17, and 19-23

IV STATUS OF AMENDMENTS (37 C.F.R. § 1.192(c)(4))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF INVENTION (37 C.F.R. § 1.192(c)(5))

A method and computer program product are provided for dynamic adaptation of a system in accordance with a contract with criteria associated therewith. As set forth in operation 303 of Figure 3 and the accompanying description, a security-related interaction between a plurality of components of the system is governed utilizing the criteria of the contract. Such components include an intrusion detection module which is subject to the governing. Further, as set forth in operation 306 of Figure 3 and the accompanying description, it is determined whether the security-related interaction between the components of the system meets the criteria of the contract. In use, the security-related interaction between the components of the system is adapted upon the criteria of the contract not being met.

VI ISSUES (37 C.F.R. § 1.192(c)(6))

Issue # 1: The Examiner has rejected Claims 1-4, 6, 7, 9, 11-14, 16, 17 and 19-23 under 35 U.S.C. 102(e) as being anticipated by Webber, Jr. (U.S. Patent No.: 6,167,378).

Issue # 2: The Examiner has rejected Claims 5 and 15 under 35 U.S.C. 103(a) as being unpatentable over Webber, Jr., as applied above, and further in view of Bigus (U.S. Patent No.: 5,745,652).

VII GROUPING OF CLAIMS (37 C.F.R. § 1.192(c)(7))

The claims of the groups below do not stand or fall together. Following is the grouping of claims. In the following section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1: Grouping of Claims –
Group #1: Claims 1-4, 6, 7, 9, 11-14, 16, 17 and 19-20.
Group #2: Claim 21.
Group #3: Claim 22.
Group #4: Claim 23.

Issue # 2: Grouping of Claims –
Group #1: Claims 5 and 15.

VIII ARGUMENTS (37 C.F.R. § 1.192(c)(8))

Issue #1:

The Examiner has rejected Claims 1-4, 6, 7, 9, 11-14, 16, 17 and 19-23 under 35 U.S.C. 102(e) as being anticipated by Webber, Jr.

Group #1: Claims 1-3, 6, 7, 11-13, 16, 17 and 20

With respect to the present grouping, the Examiner has dismissed appellant's claim amendments by stating that the claimed "security-related" interaction is met by the following excerpt from Webber.

> "An additional level of security may be provided by only activating contracts which are marked with a special authorization encryption or signature. Modification of any one element in the contract and CAP without simultaneously making the same change at all levels would immediately become evident and should readily be detected. Since the contracts are linked together, reconciliation, verification and authentication can be performed by comparing transactional data at one level for one party with the corresponding transaction for all parties at all levels. Alternatively, the CAP can operate as an exception system, by identifying deviations, rather than reviewing all transactional details." (col. 15, lines 13-24)

While such excerpt shows "security-related" activity, it fails to meet the specific context in which appellant's "security-related" interaction is claimed. As emphasized previously, appellant does not merely claim "security-related" activity, but rather "governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including an intrusion detection module which is subject to the governing."

It appears that the Examiner continues to fail to consider the full weight of appellant's claim limitations (including, in particular, the functional limitations and their relation to the claimed intrusion detection module). Webber's activation of contracts based on special authorization encryption or signatures simply does not meet appellant's claimed "governing a security-related interaction between a plurality of components" "including an intrusion detection module which is subject to the governing" "utilizing the criteria of the contract" (emphasis added).

Thus, it appears that the Examiner is trying to stretch Webber's teachings of a security technique for protecting against contract fraud and detecting the authenticity of the contracts themselves, to meet appellant's claimed invention involving governing an intrusion detection module based on a contract. This is improper, as this attempt does not anticipate each element of appellant's claimed invention (even in their broadest sense). Just by way of example, Webber fails to even suggest an "intrusion detection module," let alone a contract governed-intrusion detection module.

There is simply no teaching, disclosure and/or suggestion in Webber of any sort of governing of a security-related interaction involving an intrusion detection module utilizing the criteria of a contract.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criteria has simply not been met by the Webber reference, in view of the arguments made hereinabove.

Group #2: Claim 21

With respect to the present claim grouping, the Examiner has relied on the following excerpt to meet appellant's claimed "governing a security-related interaction between ... a plurality of intrusion detection modules, and at least one firewall which are subject to the governing" (emphasis added).

Again, the contracts of Webber govern *commercial* transactions among parties. The only mention of any security-related components is in passing, and simply does not meet appellant's claimed contract-governed security-related interaction among a plurality of intrusion detection modules, and at least one firewall.

In the latest action, the Examiner relies on the following excerpts to make a 102(e) prior art showing of the foregoing limitations:

"In accordance with one embodiment of the invention, there is provided a method for digital automation of supply chains. In a computerized system, at least one non-ratified contract is generated for a transaction in one supply chain of the supply chains, wherein the non-ratified contract has a plurality of terms. The contract is ratified and stored as a ratified contract in a database in the computerized system. If a term of the plurality of terms in the ratified contract indicates that at least one next contract is necessary for a next transaction in the supply chain, the above steps are repeated for the at least one next contract, and links between the ratified contract and the next contract are stored in the database." (col. 5, lines 4-15)

"In the preferred embodiment, the CAP and computing module utilize available secure socket layer protocols and public key encryption technology, such as that available from RSA Data security. A commercially available firewall advantageously protects and verifies a customer identifier associated with the customer, a bank identifier associated with the bank, and passwords." (col. 8, lines 59-65)

"The CAP is advantageously designed in a modular fashion so that each function is a separate independent subsystem. These independent subsystems include: security and firewalls, auditing, inventory management, management reporting, accounting, statistical logging and reporting, shipping options, distribution options, purchasing services, delivery/shipping schedules, integration of shipping with suppliers." (col. 14, lines 4-11)

Appellant asserts that the Examiner can not simply point to a general description of "firewalls" in a system with "contracts ... generated for a transaction in one supply chain of the supply chains," (see Claim 1 of Webber, for example) and then erroneously infer that such a system suggests that the contracts govern a security-related interaction between an intrusion detection module and a plurality of firewalls, in the context of the remaining claim limitations of appellant's claimed invention. To do so would require one to ignore or dismiss appellant's claim limitations, which would be improper.

Again, only appellant teaches and claims a contract-governed interaction among an "intrusion detection module" and multiple "firewalls" in the context of the

remaining claim limitations. Thus, the aforementioned anticipation criteria are clearly lacking.

Group #3: Claim 22

With respect to the present grouping, the Examiner has relied on the following excerpts from Webber to make a prior art showing of appellant's claimed "wherein the intrusion detection modules are adapted for communicating information to the analysis module for detecting intrusions."

> "Encryption or security 281, 283 may be included in the communication link 259 between the CAP 260 and the selling entities in the supply chain, and between the CAP 260 and the supply chain enterprises 277, respectively. These sellers include the CAP internet 241a, an intranet 241b, conventional retailer connection 241c, a DTC 800 number 241d, business to business communication links 241e, project management applications 241f, and government 241g, for example. Banks that are utilized as a part of financial transactions in the CAP such as the sellers bank 243 are also connected to the computing module 262 via communication link 253. A requested product 249 is provided to a customer 251 via shipping channel 261. POD is provided from the shippers for the supply chain enterprises 277 via communication link 299 to the CAP 260.
>
> Security is preferably provided on the CAP, as is illustrated in FIG. 2. For example, a seller's POS data are assigned an encrypted transactional identifier when transmitted by the computer at the seller to the CAP, thus inhibiting tampering or modification. A shipper's POD data is received at the CAP through the secure link 299 to shippers. Other information which is advantageously transmitted across a secure link to the CAP include dispute resolution data and a seller's POS or PO when received at the CAP. A different level of security can be provided for each of the above, utilizing conventional security protocols and methods. It is possible to provide a level of security corresponding to each level of risk." (col. 14, lines 44 - col. 15, line 4)

Such excerpt, however, fails to disclose, teach or even suggest intrusion detection modules, let alone communicating information to the analysis module for detecting intrusions, as claimed. Only appellant teaches and claims such a multiple intrusion detection module system that communicates with an analysis mode for

detecting intrusions, specifically, in combination with the remaining claimed features.

Thus, the aforementioned anticipation criteria are clearly lacking.

Group #4: Claim 23

With respect to the present grouping, the Examiner has relied on the foregoing excerpts from Webber to make a prior art showing of appellant's claimed "wherein information includes generalized intrusion detection objects." Such excerpt, however, fails to disclose, teach or even suggest generalized intrusion detection objects, as defined by the specification and in the context of the claims, as being communicated to the analysis mode for detecting intrusions.

Thus, the aforementioned anticipation criteria are clearly lacking.

Issue # 2

Group #1: Claims 5 and 15

The Examiner has rejected Claims 5 and 15 under 35 U.S.C. 103(a) as being unpatentable over Webber, Jr., as applied above, and further in view of Bigus.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met. Specifically, the Examiner relies on the following excerpt from Bigus to make a prior art showing of applicant's claimed "wherein the cost model criteria is based on resource utilization."

> "One of the major functions performed by computer operating system is resource allocation. Resource allocation involves giving user jobs access to the computer system's resources, such as the central processing unit (CPU), main memory, input/output devices, etc. Over the years many different resource allocation algorithms have been developed for computer systems." (col. 1, lines 42-48)

Such excerpt, however, fails to disclose, teach or even suggest resource utilization in the specific context of cost model criteria, as claimed by applicant. Thus, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art, when combined, fails to meet all of applicant's claim limitations.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

IX APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))

The text of the claims involved in the appeal is:

1. (Previously Amended) A method implemented using a computer for dynamic adaptation of a system in accordance with a contract with criteria associated therewith, comprising:

governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including an intrusion detection module which is subject to the governing;

determining whether the security-related interaction between the components of the system meets the criteria of the contract; and

adapting the security-related interaction between the components of the system upon the criteria of the contract not being met.

2. (Previously Amended) The method as recited in claim 1, wherein the security-related interaction between the components of the system is adapted by adjusting the contract.

3. (Original) The method as recited in claim 2, wherein the contract is adjusted by a method selected from the group consisting of deactivation of the contract, modification of the contract, deletion of the contract, and activation of a different contract.

4. (Original) The method as recited in claim 1, wherein the criteria of the contract include cost model criteria.

5. (Original) The method as recited in claim 4, wherein the cost model criteria is based on resource utilization.

6. (Previously Amended) The method as recited in claim 4, wherein the cost model criteria is based on performance.

7. (Original) The method as recited in claim 4, wherein the cost model criteria is based on service provisioning.

8. (Cancelled)

9. (Previously Amended) The method as recited in claim 1, wherein the components include the intrusion detection module and an analysis module.

10. (Cancelled)

11. (Previously Amended) A computer program product for dynamic adaptation of a system in accordance with a contract with criteria associated therewith, comprising:

(a) computer code for governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including an intrusion detection module which is subject to the governing;

(b) computer code for determining whether the security-related interaction between the components of the system meets the criteria of the contract; and

(c) computer code for adapting the security-related interaction between the components of the system upon the criteria of the contract not being met.

12. (Previously Amended) The computer program product as recited in claim 11, wherein the security-related interaction between the components of the system is adapted by adjusting the contract.

13. (Original) The computer program product as recited in claim 12, wherein the contract is adjusted by a method selected from the group consisting of deactivation of the contract, modification of the contract, deletion of the contract, and activation of a different contract.

14. (Original) The computer program product as recited in claim 11, wherein the criteria of the contract includes cost model criteria.

15. (Original) The computer program product as recited in claim 14, wherein the cost model criteria is based on resource utilization.

16. (Original) The computer program product as recited in claim 14, wherein the cost model criteria is based on performance.

17. (Original) The computer program product as recited in claim 14, wherein the cost model criteria is based on service provisioning.

18. (Cancelled)

19. (Previously Amended) The computer program product as recited in claim 11, wherein the components include the intrusion detection module and an analysis module.

20. (Previously Amended) An apparatus for dynamic adaptation of a system in accordance with a contract with criteria associated therewith, comprising:

a module for:

(a) governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including an intrusion detection module which is subject to the governing;

(b) determining whether the security-related interaction between the components of the system meets the criteria of the contract; and

(c) adapting the security-related interaction between the components of the system upon the criteria of the contract not being met.

21. (Previously Amended) A method implemented using a computer for dynamic adaptation of a system in accordance with a contract with criteria associated therewith, comprising:

governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including a plurality of intrusion detection modules, and at least one firewall which are subject to the governing;

determining whether the security-related interaction between the components of the system meets the criteria of the contract utilizing an analysis module; and

adapting the security-related interaction between the components of the system upon the criteria of the contract not being met utilizing the analysis module;

wherein the security-related interaction between the components of the system is adapted by adjusting the contract by a method selected from the group consisting of deactivation of the contract, modification of the contract, deletion of the contract, and activation of a different contract.

22. (Previously Presented) The method as recited in claim 21, wherein the intrusion detection modules are adapted for communicating information to the analysis module for detecting intrusions.

23. (Previously Presented) The method as recited in claim 22, wherein information includes generalized intrusion detection objects.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P002/00.056.01).

Respectfully submitted,

By: _____ Date: 6/30/04

Kevin J. Zilka
Reg. No. 41,429

Silicon Valley IP Group, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660